Opérations élémentaires sur les lignes et les colonnes exemples de décompositions d'une matrice à coefficients dans un corps, dans un anneau: applications

Plan

Remarque d'ordre général: il faut à mon avis se concentrer sur les aspects effectifs, algorithmiques. Par exemple il me semble mal à propos de disserter sur les transvections et proposer en développement la simplicité de $PSL_n(K)$ pour $n \geq 3$. Pour ouvrir le sujet, on peut introduire des opérations moins élémentaires, par exemple les matrices de Householder.

- Commencez par définir les opérations élémentaires usuelles:
  - $L_i \to L_i + \lambda L_j$ (resp. $C_i \to C_i + \lambda C_j$) est obtenu par multiplication à gauche (resp. à droite) par $T_{i,j}(\lambda)$;
  - $L_i \to \lambda L_i$ (resp. $C_i \to \lambda C_i$) est obtenu par multiplication à gauche (resp. à droite) par $D_i(\lambda)$;
  - $L_i \leftrightarrow L_j$ (resp. $C_i \leftrightarrow C_j$) est obtenue par multiplication à gauche (resp. à droite) par $P_{i,j} = I - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$.
- pour $i \neq j$, les matrices $T_{i,j}(\lambda)$ (resp. $D_i(\lambda)$) sont des matrices de transvections (resp. dilatations) élémentaires relativement à la base canonique. De manière générale les matrices de transvections (resp. dilatations) sont les matrices semblables aux matrices de transvections (resp. dilatations) élémentaires relativement à la base canonique. Une transvection (resp. dilatation) est une application linéaire u telle qu'il existe un hyperplan H tel que $u_{|H} = \mathrm{Id}_H$ et $\mathrm{Im}(u - \mathrm{Id}) \subset H$ (resp. $u \neq \mathrm{Id}$ diagonalisable).
- Sur un corps K:
  - $SL_n(K)$ est engendrée par les transvections élémentaires relativement à la base canonique: en particulier on notera que les matrices de permutation ne sont pas utiles puisqu'elles s'obtiennent à partir des matrices de transvections. Ainsi si vous introduisez les matrices de permutation et vous ferez bien, il vous faut donc les faire entrer en jeu, par exemple:
    * pour $M \in \mathbb{M}_{p,n}(K)$ de rang $r > 0$, alors il existe $Q \in SL_n(K)$ (qui est donc produit des $T_{i,j}(\lambda)$ et $\sigma \in \mathfrak{S}_n$ tels que $QMP_\sigma = \begin{pmatrix} I'_r & A \\ 0 & 0 \end{pmatrix}$ où P_σ est la matrice de permutation associée à σ et $I'_r = I_r$ si $r < p$ et $I'_r = \mathrm{diag}(1, \cdots, 1, \alpha)$ (la matrice de permutation sert à permuter les colonnes quand on moment de pivoter sur cette colonne celle-ci est combinaison linéaire des précédentes). Si on ne s'autorise pas à pivoter les colonnes on obtient une matrice échelonnée cf. plus loin
    * décomposition de Bruhat: $T(n,\mathbb{C})\backslash GL(n,\mathbb{C})/T(n,\mathbb{C}) \simeq \mathfrak{S}_n$ où $T(n,\mathbb{C})$ désigne l'ensemble des matrices triangulaires supérieures. On interprète ce résultat en termes de drapeaux: l'ensemble des classes de paires de drapeaux complets sous l'action de $GL(n,\mathbb{C})$, est en bijection avec $\mathfrak{S}_n$.
  - soit M un élément de $GL_n(K)$, alors $MD_n(\det M^{-1})$ est un produit de transvections élémentaires (moins de n^2) relativement à la base canonique
  - méthode du pivot de Gauss:
    * le calcul du rang, des déterminants;
    * résolution d'un système linéaire $AX = B$: on construit M tel que MA soit échelonnée ce qui donne des équations que doit vérifier B puis on résoud le système triangulaire avec un certain nombre de degré de liberté (théorème de Rouché-Fontené) ($2n^3/3 + o(n^3)$ opérations élémentaires) (**il faut absolument maîtriser parfaitement la question**);
    * pour le calcul de l'inverse, on utilise la méthode de Gauss-Jordan: on construit M tel que MA soit diagonale;
    * décomposition LU: on se demande, dans la méthode du pivot, si pour pivoter on a besoin d'échanger des lignes (en général oui surtout pour minimiser les erreurs d'arrondis): la condition pour que ce ne soit pas nécessaire est que $\det M^{(k)}$ soit inversible pour tout $1 \leq k \leq n$ où $M^{(k)}$ désigne le

mineur principal d'ordre k: la factorisation est alors unique si on impose à la diagonale de L d'être égale à 1. Pour la résolution des systèmes linéaires: on résoud $LY = B$ puis $UX = Y$ (on notera que le calcul de L est particulièrement simple à partir de matrices $T_{i,j}$ cf. Ciarlet p.83). On pourra mentionner le cas particulièrement simple des matrices tridiagonales (Ciarlet p.85) (qui nécessite $8n-6$ opérations) ou plus généralement des matrices bandes, dont la décomposition LU est encore de la même forme (notion de structure de données statique)

* Soit B une matrice de $\mathbb{M}_{m,n}(\mathbb{R})$ et $c \in \mathbb{R}^m$; on cherche u tel que la norme euclidienne de $Bu - c$ soit minimale (méthode des moindres carrés). On introduit la fonctionnelle

$$2J(v) := ||Bv - c||^2 - ||c||^2 = ({}^tBBv, v) - 2({}^tBc, v)$$

que l'on cherche à minimiser. La matrice symétrique ${}^tBB$ étant positive, la fonction J est convexe de sorte que l'ensemble des solutions coïncide avec celui de l'équation

$$J'(u) = {}^tBBu - {}^tBc = 0$$

On est ainsi naturellement amené à résoudre des équations $AX = B$ avec A est symétrique définie positive où on applique la décomposition de Cholesky: $A = B{}^tB$ avec B triangulaire inférieure (**attention** à priori B ne s'obtient pas par la méthode LU). Pour trouver B, on doit résoudre un système triangulaire en les coefficients de la matrice A. Si on impose aux coefficients diagonaux de B d'être strictement positifs alors on a même unicité. Résoudre le système demande alors $n^3/3+o(n^3)$ opérations élémentaires.

* le calcul du polynôme minimal;
* toute matrice est algorithmiquement semblable à une matrice de Hessenberg: dans la méthode QR si A est de Hessenberg alors tous les A_k aussi ce qui raccourcit les temps de calcul.

− sur un anneau principal:

* à la liste des opérations élémentaires on peut y adjoindre l'action des matrices $\begin{pmatrix} u & -b \\ v & a \end{pmatrix}$ de $SL_2(A)$, et de leur transposée, où $ua + vb = 1$ est une relation de Bezout que l'on obtient, sur un anneau euclidien, algorithmiquement
* on peut décrire les classes d'équivalence: en application on pourra mentionner les invariants de similitude, le théorème de la base adaptée, la classification des groupes abéliens de type fini
* pour $A = \mathbb{Z}$ ou $K[X]$, soit M un élément de $GL_n(A)$, alors $MD_n(\det M^{-1})$ est un produit de transvections élémentaires relativement à la base canonique
* réduction à la forme d'Hermite: soit $A \in \mathbb{M}_{n,k}(\mathbb{Z})$ de rang $n \leq k$, alors il existe $U \in SL_n(\mathbb{Z})$ telle que $AU = [0\ M]$ avec M triangulaire supérieure avec $0 \leq m_{i,j} < m_{i,i}$ pour $i < j < n$. La matrice M obtenue est unique et le procédé est algorithmique. (Fresnel p83)
* résolution d'un système d'équations diophantiennes.

− Si on rajoute à la liste des opérations élémentaires les matrices de Householder, on pourra citer:

* la factorisation QR où Q est unitaire et R triangulaire supérieure. Si on impose aux coefficients diagonaux de R d'être positifs ou nuls et si A est inversible, alors la factorisation $A = QR$ est unique. (sur $\mathbb{R}$, Q est orthogonale). Pour les construire on peut aussi utiliser le procédé d'orthonormalisation de Gram-Schmidt, mais il est à éviter car il engendre des erreurs d'arrondis.
* étant donnée une matrice symétrique A, il existe une matrice P produit de $(n-2)$ matrices de Householder, telle que ${}^tPAP$ soit tridiagonale (Ciarlet p.120). En appliquant alors la méthode de Givens, on obtient des valeurs approchées des valeurs propres: les polynômes caractéristiques des mineures principaux forment une suite de Sturm ce qui permet de localiser les racines aussi précisément que l'on veut par exemple par dichotomie (Ciarlet p.123).
* Méthode QR de localisation des racines: A inversible à valeurs propres toutes de modules distinctes telle qu'il existe une matrice de passage à une base de diagonalisation admettant une décomposition LU, on construit alors une suite A_k définie par récurrence $A_k = Q_kR_k = R_{k-1}Q_{k-1}$. Alors A_k converge vers la matrice diagonale des valeurs propres de A rangées par ordre décroissant de leur module.

- En application on pourra éventuellement mentionner au fil du plan sans que ce soit central:
  - si on autorise toutes les transvections et pas seulement les $T_{i,j}(\lambda)$ alors pour $1_E \neq f \in SL(E)$ qui n'est pas une affinité (resp. une affinité) alors f est produit de r (resp. $r+1$) transvections avec $r = n - \dim_K \mathrm{Ker}(f - 1_V)$ et que ce nombre est minimal.
  - connexité de $SL_n(K)$, $GL_n(\mathbb{C})$ et de $GL_n(\mathbb{R})^+$;
  - en dimension supérieure ou égale à 3, les transvections sont toutes conjuguées; on en déduit la simplicité de $SL_n(K)$. En dimension 2, pour (e_1, e_2) une base on note τ_λ la transvection définie par $\tau_\lambda(x_1e_1 + x_2e_2) = (x_1e_1 + x_2e_2) + \lambda x_2e_1$; toute transvection est conjuguée à un τ_λ et τ_λ, τ_μ sont conjuguées si et seulement si $\frac{\lambda}{\mu} \in (K^\times)^2$.

Développements

- décomposition de Bruhat
- $SL_n(K)$ est engendré par les transvections élémentaires relativement à la base canonique
- facteurs invariants
- $SL_n(A)$, pour $A = \mathbb{Z}$ ou $K[X]$, est engendré par les transvections élémentaires relativement à la base canonique (Fresnel p60)
- méthode de Gauss, Gauss-Jordan: factorisation LU
- factorisation QR et méthode QR de localisation des racines en passant par les matrices de Hesenberg

Questions

- Comment reconnaître la matrice d'une transvection (resp. dilatation)? L'ensemble des transvections est-il un groupe? Quels sont les invariants de similitude d'une transvection?
- Soit H un hyperplan d'un espace vectoriel de dimension finie V; on note $G_H = \{u \in GL(V) / \ u_{|H} = \mathrm{Id}_H\}$:
  - Montrez que tout élément de G_H est soit une transvection soit une dilatation.
  - Montrez que l'ensemble $\mathcal{T}_H$ des transvections de G_H constitue un sous-groupe distingué de G_H et que le déterminant induit un isomorphisme $G_H/\mathcal{T}_H \simeq K^\times$ et donnez la structure de G_H.
  - Montrez que les dilatations de base hyperplane quelconque engendrent $GL(V)$ alors que clairement les matrices de dilatations élémentaires relativement à la base canonique n'engendrent pas $GL(V)$.
  - Pour U un sous-groupe de $K^\times$, soit $\mathcal{G}_U := \det^{-1}(U)$. Montrez que $\mathcal{G}_U$ est engendré par les dilatations de base hyperplane quelconque de rapport $\mu \in U$.
  - On suppose car$K \neq 2$; montrez que $\mathcal{G}_{\{1,-1\}}$ est engendré par les involutions w telles que $\dim_K \mathrm{Ker}(w + 1_V) = 1$.
- Soit $1_E \neq f \in SL(E)$, on sait que f peut s'écrire comme un produit de r transvections. Montrez que $r \geq n - \dim_K \mathrm{Ker}(f - 1_V)$. (utilisez que $\mathrm{Ker}(uv - 1)$ contient l'intersection de $\mathrm{Ker}(u - 1)$ et $\mathrm{Ker}(v - 1)$)
- Proposer un algorithme pour obtenir des équations cartésiennes de l'image d'une matrice.
- Montrez que l'on peut mettre M sous la forme LU (resp. LDU) si et seulement si $\det M^{(k)} = 1$ (resp. $\det M^{(k)} \neq 0$) pour tout $1 \leq k \leq n$ où $M^{(k)}$ désigne le mineur principal d'ordre k, L (resp. U) désigne une matrice triangulaire inférieure (resp. supérieure) avec des coefficients diagonaux égaux à 1. et D désigne une matrice diagonale (applications à la résolution des systèmes linéaires: on résoud $LY = B$ puis $UX = Y$ ce qui nécessite $2n^2$ opérations).

- Soit A une matrice de $\mathbb{M}_n(K)$. On introduit la matrice N de $\mathbb{M}_{n^2,n+1}(K)$ où pour $1 \leq k \leq n+1$, son k-ième vecteur colonne est constitué des éléments de la matrice A^{k-1} pris dans un ordre prescrit une fois pour toutes. Montrez qu'il existe une matrice P de $SL_{n^2}(K)$ telle que PN soit de la forme $\begin{pmatrix} M_1 & M_2 \\ 0 & M_3 \end{pmatrix}$, où M_1 est un élément de $\mathbb{M}_{d,d+1}(K)$ "triangulaire supérieure" dont les termes "diagonaux" sont tous non nuls et donnez un moyen de calculer le polynôme minimal de A.

Exercices corrigés

Exercice 1. *(Fresnel p103) Soit H un hyperplan d'un espace vectoriel de dimension finie V; on note $G_H = \{u \in GL(V) / \ u_{|H} = \mathrm{Id}_H\}$.*

(1) Pour $u \in G_H - \{\mathrm{Id}\}$, montrez les équivalences suivantes:

(i) u est une transvection;

(ii) $\det u = 1$;

(iii) $\mathrm{Im}(u - \mathrm{Id}) \subset H$;

(iv) u est non diagonalisable

(2) Pour $u \in G_H - \{\mathrm{Id}\}$, montrez les équivalences suivantes:

(i) u est une dilatation;

(ii) $\det u \neq 1$;

(iii) il existe $v \in V$ avec $u(v) - v \notin H$;

(iv) u est diagonalisable.

(3) Montrez que tout élément de G_H est soit une transvection soit une dilatation.

(4) Montrez que l'ensemble $\mathcal{T}_H$ des transvections de G_H constitue un sous-groupe distingué de G_H et que le déterminant induit un isomorphisme $G_H/\mathcal{T}_H \simeq K^\times$ et donnez la structure de G_H.

(5) Montrez que les dilatations de base hyperplane quelconque engendrent $GL(V)$ mais que les matrices de dilatation élémentaire relativement à la base canonique n'engendrent pas $GL(V)$.

(6) Pour U un sous-groupe de $K^\times$, soit $\mathcal{G}_U := \det^{-1}(U)$. Montrez que $\mathcal{G}_U$ est engendré par les dilatations de base hyperplane quelconque de rapport $\mu \in U$.

(7) On suppose $\mathrm{car} K \neq 2$*; montrez que* $\mathcal{G}_{\{1,-1\}}$ *est engendré par les involutions w telles que* $\dim_K \mathrm{Ker}(w + \mathrm{Id}) = 1$.

Preuve : (1) (i) implique (ii): on choisit une base de H que l'on complète en une base de E; la matrice de u dans cette base est alors triangulaire supérieure avec des 1 sur la diagonale.

(ii) implique (iii): soit $v \in E$ n'appartenant pas à H de sorte que si $(e_1, \cdots, e_{n-1})$ est une base de H, la matrice de u dans la base $(e_1, \cdots, e_{n-1}, v)$ est triangulaire supérieure avec ses $n-1$-premiers termes diagonaux égaux à 1. Si le déterminant est égal à 1, on a alors $u(v) - v \in H$ et $u(e_i) - e_i \in H$ pour tout $1 \leq i \leq n-1$ et donc le résultat par linéarité.

(iii) implique (iv): dans la base définie précédemment si $\mathrm{Im}(u - \mathrm{Id}) \subset H$ alors, les coefficients diagonaux de la matrice de u sont tous égaux à 1. Si u était diagonalisable il serait égal à l'identité ce qui n'est pas par hypothèse.

(iv) implique (i): l'espace propre associée à la valeur propre 1 est de dimension supérieure ou égale à 1 car $u \in G_H$; u étant différent de l'identité cette dimension est exactement $n-1$ et comme elle est non diagonalisable 1 est son unique valeur propre. Soit alors e_n un élément de $\mathrm{Ker}(u - \mathrm{Id})^2$ n'appartenant pas à $\mathrm{Ker}(u - \mathrm{Id})$ et soit $0 \neq e_{n-1} = u(e_n) - e_n \in \mathrm{Ker}(u - \mathrm{Id}) =: H$. On complète e_{n-1} en une base $e_1, \cdots, e_{n-1}$ de H de sorte que la matrice de u dans la base $(e_1, \cdots, e_n)$ est égale à $T_{n-1,n}$.

(2) (i) implique (ii): c'est clair

(ii) implique (iii): H est inclu dans le sous-espace propre associé à la valeur propre 1. Comme $\det u \neq 1$, on en déduit que la dernière valeur propre est différente de 1, la valeur propre associée vérifie alors la propriété demandée.

(iii) implique (iv): soit $(e_1, \cdots, e_{n-1})$ une base de H et soit e_n tel que $u(e_n) - e_n \notin H$. On a alors $e_n \notin H$ de sorte que $(e_1, \cdots, e_n)$ est une base de V. On en déduit alors que u admet une valeur propre λ différente de 1 et que le sous-espace propre associée à la valeur propre 1 (resp. λ) est de dimension supérieure ou égale à $n-1$ (resp. 1), on en déduit donc les égalités et que u est diagonalisable.

(iv) implique (i): dans une base de diagonalisation la matrice de u est de la forme $D_n(\lambda)$.

(3) un élément u de G_H est soit de déterminant 1 (resp. non diagonalisable) ou de déterminant différent de 1 (resp. diagonalisable) et donc d'après ce qui précède soit une transvection soit une dilatation.

(4) Pour τ une transvection de base hyperplane H et pour u un automorphisme alors $u\tau u^{-1}$ est une transvection de base hyperplane $u(H)$. Si u appartient à G_H, on a en particulier $u(H) = H$ et donc $\mathcal{T}_H$ est distingué dans G_H. D'après (1), le noyau du déterminant est égal à $\mathcal{T}_H$; le résultat découle alors de la surjectivité du déterminant.

Par ailleurs $\mathcal{T}_H$ est en bijection avec H: pour v un vecteur fixé n'appartenant pas à H, à une transvection τ de G_H, on lui associe $\tau(v) - v$. Par ailleurs l'ensemble des dilatations telles que $u(v) = \lambda v$ constitue un relèvement de $\det G_H/\mathcal{T}_H \simeq K^\times$ de sorte que G_H est le produit semi-direct $H \rtimes_\Psi K^\times$ où $\Psi : K^\times \longrightarrow GL(H)$ définie par $\Psi(\lambda) = \lambda^{-1}\mathrm{Id}$.

(5) Remarquons que si τ (resp. u) est une transvection (resp. dilatation de rapport μ) de G_H alors $\tau \circ u$ est une dilatation v de rapport μ de G_H (le déterminant est égal à μ). Ainsi on a $\tau = u^{-1}v$ de sorte que le groupe engendré par les dilatations est $GL(V)$ car pour tout élément g de $GL(V)$, $gD_n(\det g^{-1})$ est un produit de transposition.

(6) C'est la même démonstration que dans (5).

(7) Les dilatations de rapport ± 1 sont des involutions w telles que $\mathrm{Ker}(w+\mathrm{Id})$ est de dimension 1. Réciproquement une involution est diagonalisable avec pour valeurs propres ± 1. Si $\mathrm{Ker}(w+\mathrm{Id})$ est de dimension 1 alors $\mathrm{Ker}(w-\mathrm{Id})$ est de dimension $n-1$ ce qui en fait une dilatation. On conclut donc via (6).

Exercice 2. *Soit E un K-espace vectoriel de dimension n. Un automorphisme f est appelé une* ***affinité ou dilatation de base*** *E_1* ***de direction*** *$E_2 \neq (0)$ et de rapport $\lambda \neq 1$ si $E = E_1 \oplus E_2$ telle que $f_{|E_1} = \mathrm{Id}_{E_1}$ et $f_{|E_2} = \lambda \mathrm{Id}_{E_2}$.*

(1) Montrez que f est une affinité si et seulement si son polynôme minimal est de la forme $(X-1)(X-\lambda)$ pour $\lambda \neq 1$.

(2) Soit $1_E \neq f \in SL(E)$ qui n'est pas une affinité (resp. une affinité). Montrez que f est produit de r (resp. $r+1$) transvections avec $r = n - \dim_K \mathrm{Ker}(f - 1_V)$ et que ce nombre est minimal.

Preuve : cf. Fresnel p.104

Exercice 3. *(Fresnel p.127) Soit A une matrice de $\mathbb{M}_n(K)$. On introduit la matrice N de $\mathbb{M}_{n^2,n+1}(K)$ où pour $1 \leq k \leq n+1$, son k-ième vecteur colonne est constitué des éléments de la matrice A^{k-1} pris dans un ordre prescrit une fois pour toutes. Montrez qu'il existe une matrice P de $SL_{n^2}(K)$ telle que PN soit de la forme $\begin{pmatrix} M_1 & M_2 \\ 0 & M_3 \end{pmatrix}$, où M_1 est un élément de $\mathbb{M}_{d,d+1}(K)$ "triangulaire supérieure" dont les termes "diagonaux" sont tous non nuls et donnez un moyen de calculer le polynôme minimal*

Preuve : L'existence de S découle du pivot de Gauss par opérations sur les lignes. Ainsi les $d+1$-premières colonnes de $N' = SN$ sont liées soit ${}^t(u_0, \cdots, u_{d-1}, -1, 0, \cdots, 0)$ un vecteur du noyau de N' et donc aussi de N car S est inversible. En notant C_i les colonnes de N, on a donc $C_d = u_0 C_0 + \cdots + u_{d-1}C_{d-1}$ et donc $A^d - u_{d-1}A^{d-1} - \cdots - u_0 \mathrm{Id} = 0$. Supposons qu'il existe un polynôme annulateur de degré inférieur ou égal à $d-1$, de sorte que les $d-1$ première colonnes de N sont liées et donc aussi celles de N' ce qui n'est pas, de sorte que $X^d - u_{d-1}X^{d-1} - \cdots - u_0$ est bien le polynôme minimal de A.

Exercice 4. *Soit M une matrice de $\mathbb{M}_n(\mathbb{R})$; les lettres L, L' (resp. U, U') désigne des matrices triangulaires inférieures (resp. supérieures) avec des coefficients diagonaux égaux à 1. La lettre D désigne une matrice diagonale.*

(1) Montrez que l'on peut mettre M sous la forme LU (resp. LDU) si et seulement si $\det M^{(k)} = 1$ (resp. $\det M^{(k)} \neq 0$) pour tout $1 \leq k \leq n$ où $M^{(k)}$ désigne le mineur principal d'ordre k.

(2) Ecrire la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *sous la forme $U'LU$. Trouvez une matrice de $\mathbb{M}_2(\mathbb{R})$ qui ne peut pas s'écrire sous la forme LDU où D désigne une matrice diagonale.*

(3) On note M_k la matrice obtenue à partir de M en substituant sa dernière ligne à sa ligne d'indice k. On suppose que $\det M_k^{(k)} \neq 0$ pour tout $1 \leq k \leq n$. Montrez que l'on peut mettre, de manière unique, M sous la forme $U'LU$ où U, U' ont des coefficients nuls en dehors de sa diagonale et de la dernière colonne.

(4) Soit $M \in GL_n(\mathbb{R})$, montrez qu'il existe U' avec $n-1$ coefficients nuls sur sa dernière colonne telle que les k première lignes de $(U'M)^{(k+1)}$ sont indépendantes pour tout $k < n$.

(5) Montrez que toute matrice M de déterminant n peut se mettre sous la forme $L'U'LU$ où L' a ses coefficients nuls hors de sa diagonale et de sa dernière ligne.

Preuve : (1) La preuve est identique dans le cas respé, on traite la décomposition LU. Supposons par récurrence que $M^{(n-1)} = LU$. On a

$$M = \begin{pmatrix} LU & A \\ B & m \end{pmatrix} = \begin{pmatrix} L & 0 \\ BU^{-1} & 1 \end{pmatrix} \begin{pmatrix} U & L^{-1}A \\ 0 & m' \end{pmatrix}$$

où $m' = m - BU^{-1}L^{-1}A$. Par passage au déterminant on a $m' = 1$ d'où le résultat. Pour l'unicité si $LU = L'U'$ alors $L'^{-1}L = U'U^{-1}$ qui est forcément égale à l'identité.

(2) La décomposition

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & -\tan(\theta/2) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \sin\theta & 1 \end{pmatrix} \begin{pmatrix} 1 & -\tan(\theta/2) \\ 0 & 1 \end{pmatrix}$$

est utilisée pour implémenter la rotation des images numériques. La matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ne peut pas s'écrire sous la forme LDU.

(3) On note $(c_1, \cdots, c_{n-1}, 1)$ les coefficients de la dernière colonne de U'^{-1}. Par multi-linéarité du déterminant on a

$$\det(U'^{-1}M)^{(k)} = \det M^{(k)} + \sum_{j=1}^{k} c_j M_j^{(k)}$$

Les équations $\det(U'^{-1}M)^{(k)} = 1$ pour $1 \leq k \leq n-1$ forment un système triangulaire inversible car $\det M_k^{(k)} \neq 0$, il a donc une unique solution et $(U'^{-1}M)^{(k)} = LU$ d'après (1).

(4) On démontre cette propriété pour tout $k \leq r$ par récurrence sur $r < n$ en utilisant que les matrices U' forment un groupe. On note $U_{k,k}$ la matrice identité et $U_{k,l}$ $(k < l < n)$la matrice qui par multiplication à gauche ajoute la ligne l à la ligne k. On extrait de M les matrices supérieures gauche $M^{(i,j)} \in \mathbb{M}_{i,j}(\mathbb{R})$.

Pour $r = 1$, $\mathrm{rg} M^{(n,2)}) = 2$ garantit $\mathrm{rg} M^{(n-1,2)} \geq 1$. Si la première ligne de $M^{(n-1,2)}$ est nulle on note $l > 1$ l'indice d'une ligne non nulle, sinon on pose $l = 1$. La matrice $U' = U_{1,l}$ convient, i.e. la première ligne de $(U_{1,l}M)^{(2)}$ n'est pas nulle.

On suppose que M satisfait la propriété pour tout $k \leq r-1$ si bien que les $r-1$ premières lignes de $M^{(n-1,r+1)}$ sont indépendantes. Par ailleurs, $\mathrm{rg} M^{(n-1,r+1)} \geq \mathrm{rg} M^{(n,r+1)} - 1 = r$. On choisit $U' = U_{r,l}$ où $l = r$ si la r-ième ligne de $M^{(n-1,r+1)}$ est indépendante des précédentes et $l > r$ est l'indice d'une ligne indépendante sinon. Les r premières lignes de $(U'M)^{(k+1)}$ sont alors indépendantes pour tout $k \leq r$.

(5) Soit U_0 la matrice obtenue en appliquant la question précédente à M. On remarque que $L_0 = L'^{-1}$ est de la même forme que L' et donc que U_0 et L_0 commutent. Pour tout vecteur v indépendant des $(n-1)$-premières lignes de M, on peut choisir L_0 telle que la multiplication à gauche de L_0 sur M change la dernière ligne de M en v. Par construction de U_0, il est possible de choisir les coefficients de v successivement pour que L_0U_0M satisfasse les hypothèses de la question (3). En notant U_1 la matrice U' obtenue en appliquant la question (3) à L_0U_0M on obtient $U_0L_0M = L_0U_0M = U_1LU$. On conclut en posant $U' = U_0^{-1}U_1$.

Exercice 5. *Soit (e_1, e_2, e_3) la base canonique de $\mathbb{Z}^3$ et soit $L \subset \mathbb{Z}^3$ le sous-groupe engendré par les vecteurs*

$$e_1' := 2e_1 - e_2 + e_3, \quad e_2' := e_1 + 4e_2 - e_3, \quad e_3' := 3e_1 - e_2 - e_3$$

Trouver une base adaptée au sous-module L de $\mathbb{Z}^3$ et décrire $\mathbb{Z}^3/L$. Peut-on obtenir ce dernier résultat de manière plus rapide ?

Preuve : *Convention d'écriture de produits de matrices*: on opère sur les lignes d'une matrice A en la multipliant à gauche par des matrices L_i et on présente le calcul de la manière suivante où I désigne la matrice identité:

$$\begin{array}{ccc} & I & A \\ L_1 & L_1 & L_1A \\ L_2 & L_2L_1 & L_2L_1A \\ \cdots & \cdots & \cdots \end{array}$$

De même pour opérer sur les colonnes d'une matrice A on la multiplie à droite par des matrices R_i et on présente le calcul comme suit

$$\begin{array}{cccc} & R_1 & R_2 & \cdots \\ A & AR_1 & AR_2 & \cdots \\ I & R_1 & R_1R_2 & \cdots \end{array}$$

On écrit la matrice de passage

$$\begin{pmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 1 & -1 & -1 \end{pmatrix}$$

et on commence par opérer sur les lignes

$$\begin{array}{ccc}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 1 & -1 & -1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & 3 \\ 1 & -1 & -1 \\ 0 & -3 & 2 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 0 & -1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & -1 \\ 0 & -3 & -5 \\ 0 & -3 & 2 \end{pmatrix}
\end{array}$$

puis sur les colonnes

$$\begin{array}{cccc}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & -1 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & -1 & -1 \\ 0 & -3 & -5 \\ 0 & -3 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 3 & 2 \\ 0 & 3 & -5 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 3 & -5 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 8 & -21 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 2 \\ 0 & -2 & 5 \\ 0 & 1 & -3 \end{pmatrix}
\end{array}$$

puis finalement

$$\begin{array}{ccc}
 & \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 0 & -1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 8 & -21 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -8 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 8 & -1 & -15 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -21 \end{pmatrix}
\end{array}$$

La base adaptée est alors donnée par

$f_1 = e'_1 = \begin{pmatrix} 2 & -1 & 1 \end{pmatrix} \quad f_2 = -e'_1 - 2e'_2 + e'_3 = \begin{pmatrix} -1 & -8 & 0 \end{pmatrix}$

$$21f_3 = 2e'_1 + 5e'_2 - 3e'_3 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$$

Comme vérification des calculs précédents on peut vérifier que le produit

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 8 & -1 & -15 \end{pmatrix} \begin{pmatrix} 2 & -1 & 0 \\ -1 & -8 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

est la matrice identité.

On en déduit alors que $\mathbb{Z}^3/L \simeq \mathbb{Z}/21\mathbb{Z}$. Le calcul du déterminant de la matrice de départ nous aurait donc donné 21 qui est donc égal au produit des facteurs invariants ce qui impose $a_1 = a_2 = 1$ et $a_3 = 21 = 3.7$ et donc $\mathbb{Z}^3/L \simeq \mathbb{Z}/21\mathbb{Z}$. On pourra se référer à l'exercice suivant.

Exercice 6. *Soit $x = (n_1, \dots, n_p) \in \mathbb{Z}^p$.*
a) Montrer que les conditions suivantes sont équivalentes :

1. *PGCD $(n_1, \dots, n_p) = 1$*
2. *Il existe $A \in SL_p(\mathbb{Z})$ telle que $A^t x =^t (1, 0, \dots, 0)$*
3. *Le vecteur x fait partie d'une base de $\mathbb{Z}^p$.*

b) On pose $p = 4$ et $x = (10, 6, 7, 11)$. Compléter x en une base de $\mathbb{Z}^4$.

Preuve : (i) implique (ii): le résultat se démontre par récurrence; la première étape du calcul est la suivante:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \cdots & u & v \\ 0 & \cdots & -n_r/(n_r, n_{r-1}) & n_{r-1}/(n_r, n_{r-1}) \end{pmatrix} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ (n_r, n_{r-1}) \\ 0 \end{pmatrix}$$

où u et v sont les coefficients de Bezout entre n_{r-1} et n_r: $un_{r-1} + vn_r = (n_r, n_{r-1})$.

On considère $f : \mathbb{Z}^r \longrightarrow \mathbb{Z}$ défini par $f(a_1, \cdots, a_r) = a_1 n_1 + \cdots + a_r n_r$. Le théorème de la base adaptée, nous assure l'existence d'une base $(e_1, \cdots, e_n)$ de $\mathbb{Z}^n$ tel que $\operatorname{Ker} \phi = \mathbb{Z}a_1 e_1 \oplus \cdots \oplus \mathbb{Z}a_r e_r$ avec $a_i | a_{i+1}$ dans $\mathbb{Z}$ que l'on appelle les facteurs invariants de $\mathbb{Z}^n / \operatorname{Ker} \phi$; on a en outre que les a_i sont tous égaux à 1 pour $1 \leq i < r$ et $a_r = 0$ (par un argument de dimension). Ainsi si on note A transposée de la matrice de passage de la base $(e_r, e_{r-1}, \cdots, e_1)$ dans la base canonique, on a $A \in SL_r(\mathbb{Z})$ et $A \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

(ii) implique (iii): il est évident que la famille $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = A^{-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, A^{-1} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots, A^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ forme une base de $\mathbb{Z}^n$.

(iii) implique (i): soit $e_2, \cdots, e_r$ une famille qui complète $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$ en une base et on note A la matrice de passage de cette base dans la base canonique; on calcule le déterminant de A en le développant par rapport à la première colonne de sorte que celui-ci est divisible par le pgcd des n_i qui est donc égal à 1 car $\det A = \pm 1$.

Exemples: le premier cas est simple car on a la relation $7 - 6 = 1$ de sorte que la matrice suivante est de déterminant -11

$$\begin{pmatrix} 10 & 6 & 7 & 11 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

de sorte que les 4 vecteurs colonnes de la transposée de la matrice ci-dessus constituent une base de $\mathbb{Z}^4$.
Dans le deuxième exemple on a la relation de Bezout: $1 = 6.6 - 2.10 - 15$. On cherche donc 6 coefficients a, b, c, d, e, f tels que $cf - de = 6$, $af - be = 2$ et $ad - bc = -1$. Par exemple la matrice suivante convient

$$\begin{pmatrix} 6 & 1 & 0 \\ 10 & 0 & -1 \\ 15 & 6 & 2 \end{pmatrix}$$

Exercice 7. *Résoudre dans $\mathbb{Z}^4$ le système*

$$\begin{pmatrix} 3 & 2 & 3 & 4 \\ 1 & -2 & 1 & -1 \end{pmatrix} X = \begin{pmatrix} -8 \\ -3 \end{pmatrix}$$

Preuve : Résoudre cette équation revient comme d'habitude à trouver une solution particulière, puis déterminer le noyau de la matrice en question. On fait d'une pierre deux coups en cherchant les éléments du noyau de la matrice

$$\begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix}$$

dont la dernière coordonnées est 1. Les calculs sont les suivants où l'on calcule à chaque étape la matrice de passage:

$$\begin{array}{ccc}
 & \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ -3 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix} & \begin{pmatrix} \underline{0} & 1 & 3 & 4 & 8 \\ 8 & 3 & 1 & -1 & 3 \end{pmatrix} & \begin{pmatrix} 0 & \underline{0} & 1 & 4 & 8 \\ 8 & 8 & 3 & -1 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ -3 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 3 & 1 & 0 & 0 \\ -3 & -3 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}
\end{array}$$

$$\begin{array}{ccc}
\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 8 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 0 & 0 & \underline{0} & 1 & 8 \\ 8 & 8 & 13 & 3 & 3 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & \underline{0} & 1 \\ 8 & 8 & 13 & 21 & 3 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ \underline{0} & 8 & 13 & 21 & 3 \end{pmatrix} \\
\begin{pmatrix} 2 & 3 & 4 & 1 & 0 \\ -3 & -3 & -4 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 3 & 4 & 8 & 1 \\ -3 & -3 & -4 & -8 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} -1 & 3 & 4 & 8 & 1 \\ 0 & -3 & -4 & -8 & -1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}
\end{array}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 13 & 5 & 0 & 0 \\ 0 & -8 & -3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 21 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & \underline{0} & 1 & 21 & 3 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \underline{0} & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 7 & 3 & 8 & 1 \\ 0 & -7 & -3 & -8 & -1 \\ 1 & -13 & -5 & 0 & 0 \\ 0 & 8 & 3 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix} \qquad \begin{pmatrix} -1 & 7 & 55 & 3 & 1 \\ 0 & -7 & -55 & -3 & -1 \\ 1 & -13 & -105 & -5 & 0 \\ 0 & 8 & 63 & 3 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Ainsi une solution particulière est $X_0 = (55, -55, -105, 63)$ et l'ensemble des solutions est l'ensemble $X_0 + \alpha(-1, 0, 1, 0, 0) + \beta(7, -7, -13, 8)$ où α, β décrivent $\mathbb{Z}$.

Exercice 8. *Soient n un entier positif et $G \subset \mathbb{Z}^n$ un sous-groupe de rang n. Soit $(g_1, \cdots, g_n)$ une base de G ; on note M la matrice de passage de cette base dans la base canonique de $\mathbb{Z}^n$.*

(i) Montrer que le groupe $\mathbb{Z}^n/G$ est fini.

(ii) Montrer que card($(\mathbb{Z}^n/G)$) $= |\det M|$.

(iii) Soit H un groupe abélien engendré par trois éléments h_1, h_2, h_3 soumis aux relations

$$3h_1 + h_2 + h_3 = 0$$

$$25h_1 + 8h_2 + 10h_3 = 0$$

$$46h_1 + 20h_2 + 11h_3 = 0$$

Montrer que card(H) $= 19$ puis que $H \simeq \mathbb{Z}/19\mathbb{Z}$. Quelle généralisation cela suggère-t-il ?

(iv) Triangulariser la matrice

$$\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$$

en multipliant à droite par une matrice de $SL_3(\mathbb{Z})$ que l'on précisera.

(v) En déduire un isomorphisme $\varphi : H \simeq \mathbb{Z}/19\mathbb{Z}$ et préciser les valeurs de $\varphi(h_1), \varphi(h_2), \varphi(h_3)$.

Preuve :

(i) Le théorème de la base adaptée fournit une base $(f_1, \cdots, f_n)$ de $\mathbb{Z}^n$ ainsi que des entiers $1 < a_1 | \cdots | a_n \neq 0$ tels que $(a_1 f_1, \cdots, a_n f_n)$ soit une base de G. On obtient alors $\mathbb{Z}^n/G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$.

(ii) D'après ce qui précède, on a donc $\mathrm{card}(\mathbb{Z}^n/G) = \prod_{i=1}^n a_i$ qui est donc égal à $\det M$.

(iii) Soit $M = \begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$ de sorte que $M \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ Il existe alors des matrices $L, R \in GL_3(\mathbb{Z})$ telles que $M = L\mathrm{diag}(a_1, a_2, a_3)R$ avec $a_1|a_2|a_3$. En outre si on pose $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} := R \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$, H est aussi engendré par h'_1, h'_2, h'_3 et l'équation $L\mathrm{diag}(a_1, a_2, a_3) \begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ est équivalente à

$$\begin{cases} a_1 h'_1 = 0 \\ a_2 h'_2 = 0 \\ a_3 h'_3 = 0 \end{cases}$$

et donc $H \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \mathbb{Z}/a_3\mathbb{Z}$, avec $a_1.a_2.a_3 = \det M$. L'énoncé nous suggère de simplement calculer $\det M$; on vérifie aisément qu'il est égal à -19 (cf. (iv) ci-après) comme annoncé. On obtient alors $a_1 = a_2 = 1$ et $a_3 = 19$.

De manière général si la décomposition en facteurs premiers de $\det M$ ne fait apparaître aucune multiplicité (i.e. $p^2 \not| \det M$ pour tout premier p), alors tous les a_i sont égaux à 1 sauf le dernier égal à $\det M$ et le groupe quotient est alors cyclique.

(iv) On calcule

$$
\begin{array}{cccc}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix} \\
\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix} & \begin{pmatrix} 3 & 1 & 0 \\ 25 & 8 & 2 \\ 46 & 20 & -9 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 8 & -1 & 2 \\ 20 & 14 & -9 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ 20 & -14 & -19 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix}
\end{array}
$$

(v) On a $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$ ce qui s'inverse facilement (la matrice est "triangulaire") soit $h_3 = h'_3$, $h_2 + 2h_3 = h'_1$ soit $h_2 = h'_1 - 2h'_3$ et $h_1 - 3h_2 - 5h_3 = h'_2$ soit $h_1 = 3h'_1 + h'_2 - h'_3$. Comme $\psi(h'_1) = \psi(h'_2) = 0$ et $\psi(h'_3) = 1$, on obtient $\psi(h_1) = -1$, $\psi(h_2) = -2$ et $\psi(h_3) = 1$.